Science Applications International Corporation
An Employee-Owned Company

March 11, 1998

TO: Deputy Secretary of Defense

THROUGH: Under Secretary of Defense for Acquisition and Technology
Assistant Secretary of the Air Force for Acquisition and nominee for Assistant Secretary of Defense for Command, Control, Communications, and Intelligence

13 MAR 98

SUBJECT: DRI Directive #17 Report

The attached report, "A Recommended Blueprint for the ASD(C3I) and C3I in response to DRI Directive #17," was prepared in response to your request to me earlier this year.

The recommendations contained in this report address key organizational issues and were predicated on helping the Department move towards its stated goal of obtaining Information Superiority as called for in *Joint Vision 2010*.

It is impractical to append the volume of material the Blueprint Team collected to this report. However, if you have any questions on the content of the report I would be happy to discuss them with you or your staff.

It has been an honor to support you and the Secretary with the Defense Reform Initiative. I stand ready to assist you in the implementation of the reforms necessary to the future success of the Department.

Sincerely,

Duane P. Andrews
Executive Vice President

#914

1710 Goodridge Drive, P.O. Box 1303, McLean, Virginia 22102 (703) 821-4300
Other SAIC Offices: Albuquerque, Boston, Colorado Springs, Dayton, Huntsville, Las Vegas, Los Angeles, Oak Ridge, Orlando, Palo Alto, San Diego, Seattle, and Tucson

A Recommended Blueprint
for the
ASD(C3I) and CIO
in response to DRI Directive #17

March 11, 1998

Submitted by
Duane P. Andrews

The Team charged by the Deputy Secretary of Defense to develop a Blueprint to merge C4ISR systems into the Office of the Under Secretary of Defense for Acquisition and Technology found that the personnel in OASD(C3I) would benefit greatly if they shared a common, clear vision of the Department's objectives and had the support of strong leadership.

The following recommendations satisfy the intent of the DRI to refocus the C3I organization on core OSD functions; tighten coordination between the acquisition of weapon systems, C4ISR systems, and supporting information technology; more effectively integrate Information Operations and information assurance with the Department's information activities; are consistent with the statutory responsibilities of the CIO, DoD [Specific responsibilities of the head of the agency and of the CIO concerning information technology are spelled out in Division E of the Clinger-Cohen Act of 1996 also known by the division title as the Information Technology Management Reform Act of 1996 or ITMRA.]; and, put the Department on a path towards achieving information superiority.

Those recommendations related to organizational matters are consistent with Deputy Secretary of Defense memorandum, "Office of the Assistant of Defense for C3I," dated February 5, 1998, which promulgated the decision to retain an integral C3I Secretariat.

The conclusions and recommendations that follow are proceeded by an explanation of the factors that led to each specific recommendation. The findings, conclusions and recommendations contained herein are advisory to the Department of Defense.

INFORMATION SUPERIORITY

The Defense Reform Initiative (DRI)[1] called for the realignment of the functions of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I). The DRI recommended the intelligence functions be transferred to a newly established Assistant Secretary of Defense for Intelligence (ASD(I)) and the C3 and intelligence acquisition functions be transferred to the Undersecretary of Defense for Acquisition and Technology (USD(A&T)). In addition, the USD(A&T) would be designated as the Chief Information Officer (CIO) of the Department of Defense.

The Study Team endorses the Department's decision that the intent of the DRI for improved policy formulation and oversight could largely be met by aligning the oversight of C4ISR systems under the USD(A&T). This brings together the acquisition activities of the Department and provide a closer linkage between the acquisition of weapon systems, C4ISR systems and the information technology activities of the Department.

Under this construct, the Secretariat for C3I will be retained. The team also endorses the decision that the official designated as the assistant secretary for C3I also be designated as the CIO, DoD[2]. In order to comply with the requirement of ITMRA that the CIO report

---

[1] Defense Reform Initiative: The Business Strategy for Defense in the 21st Century, November 1997

[2] While almost all functions in the Department of Defense depend upon information, some of the of the most information-intense activities of the Department are associated with the functions of command, control, computers, intelligence, surveillance, and reconnaissance. These functional activities are under the purview of the C3I Secretariat. Since 1990 the responsibility for the oversight of the information

directly to the head of the agency,[3] and to ensure the intelligence function reports directly to the Secretary and Deputy Secretary of Defense as recommended by the DRI, the official designated as the ASD(C3I) will report directly to the Secretary and Deputy Secretary of Defense for intelligence and CIO matters and to the USD(A&T) for C4ISR system acquisition matters.

Given the thrusts of the Clinger-Cohen Act of 1996 and of Joint Vision 2010, it would be appropriate for the Secretary of Defense to designate the ASD(C3I) as the principle staff assistant for information superiority[4]. Further, it may be beneficial to explore with the national security committees of the Congress the benefits of changing the name and function of the ASD(C3I) to the Assistant Secretary of Defense for Information Superiority (ASD(IS)) with his or her principal duty being the overall supervision of the information superiority affairs of the Department of Defense.

Recommendation #1
The Secretary of Defense, having assigned the function of Chief Information Officer of the Department of Defense (CIO, DoD) to the official designated as the assistant secretary of defense for command, control, communications, and intelligence (ASD(C3I), designate the ASD(C3I) as his principal staff assistant for Information Superiority.

ITMRA Sections 5123, Capital Planning and Investment, subsection (b)(1) and (2) requires the selection of information technology investments of the Department of Defense to be integrated with the processes for making budget, financial, and program management decisions and Section 5125, Agency Chief Information Officer, subsection (b)(1) charges the CIO with "providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed ... in a manner that implements the polices and procedures of [ITMRA] and the priorities established by the head of the agency. To that end, the CIO should serve as a member of the Defense Resources Board to address all matters affecting the achievement of information superiority and the objectives of the Secretary of Defense.

Recommendation #2
The Secretary of Defense direct that the ASD(C3I) serve as a member of the Defense Resources Board.

---

management activities of the Department, as delegated to the Department by the Administrator of the General Services Administration under the Brooks Act, were also assigned to the C3I Secretariat. The Clinger-Cohen Act of 1996 cancelled the Brooks Act and assigned authority for information technology acquisition to the heads of the executive agencies and expanded the responsibilities of the Chief Information Officer (CIO) in the executive agencies of the Federal government.

[3] 44 USC Sec. 3506 as amended by Pub L. 104-106 (ITMRA) requires the CIO to report directly to the agency head.

[4] Title 10, Sec.138 requires the ASD(C3I)'s "principal duty be the overall supervision of the command, control, communications, and intelligence affairs of he Department of Defense." ITMRA Sec 5125 requires the CIO "have information resource management duties as that official's primary duty." Both are necessary to the attainment of information superiority.

CONSOLIDATION OF FUNCTIONS

The proposed Blueprint organization of the office of the ASD(C3I) and CIO support staff achieve the program efficiencies and program devolvements directed by the Defense Reform Initiative. Consistent with the intent of the DRI, collection capability requirements for intelligence systems would be validated within the office headed by the DASD(I&S). Further the DASD(I&S) would provide the single interface to the NFIP and perform cross-budget analysis of NFIP, JMIP, and TIARA programs.

To ensure a single authoritative spokesman for Defense intelligence matters and gain efficiencies in determining customer satisfaction with intelligence support, the team recommends the transfer to the C3I Secretariat, under the DASD(I&S), the staff of the Special Assistant to the Secretary of Defense for Intelligence Policy, hereafter referred to as the Intelligence Oversight office, the Special Advisory Staff, and responsibility for SAP/SAR Policy.

The National Defense Authorization Act for Fiscal Year 1998 requires the Secretary of Defense to transfer system acquisition and program management from the Defense Airborne and Reconnaissance Office (DARO) to the military departments and to restrict the OSD functions to policy formulation and oversight of airborne reconnaissance programs.

The DRI proposed that responsibility for ISR systems be transferred to an office under the USD(A&T). The team concurs with the intent of the DRI and recommends that policy and oversight functions for intelligence, reconnaissance and surveillance systems can best be carried out in a coordinated process where trade-offs can be made between intelligence, surveillance, reconnaissance and tactical warning and attack assessment (TW/AA) systems whether airborne, space-based (both government and commercial) or unattended ground sensors.

An analytic capability to conduct C4ISR system trade-offs should be maintained within the C3I Secretariat, including a sufficient budget to contract for the highly technical analysis and the close integration with the development of the C4ISR nodes embedded in weapon systems and the information technology activities of the CIO. This integrated analytic capability is needed to ensure the efficient and effective C4ISR system capability required for information superiority over any potential adversary.

Oversight of ISR systems and trade-off analysis between alternative system solutions would be conducted under the DASD(C4ISR). The individuals conducting such analysis will coordinate closely with the staff of the DASD(I&S) on intelligence, intelligence-related, surveillance, and reconnaissance systems. The DASD(I&S) will lead the trade-off analysis of NFIP programs and will obtain analytic support for technical and system matters from the DASD(C4ISR).

The Blueprint proposes to enhance the status of Information Operations and Information Assurance by establishing an identified Information Operations office. This office will increase the Department's focus on information superiority and provide oversight of the Defense information Assurance Program. Consistent with the intent of the DRI, the electronic warfare/electronic combat (EW/EC), tactical command and control

countermeasures (C2CM), and Combat ID functions that are currently assigned within the A&T Secretariat should be realigned under the ASD(C3I) to facilitate the integration and cross-program analysis of C4ISR and space systems and the integration of EW/EC and C2CM activities with Information Operations. The ASD(C3I) should consider aligning personnel and physical security with this office.

Recommendation #3
The Secretary of Defense move the Intelligence Oversight function and staff, Special Advisory Staff, and SAP/SAR Security Policy to the C3I Secretariat.

Recommendation #4
The USD(A&T), consistent with the recommendation contained in the DRI, transfer the policy and oversight functions currently in the Defense Airborne and Reconnaissance Office, in the office of the Deputy Undersecretary of Space, and in the office of Strategic and Tactical Systems as relates to electronic warfare (EW), electronic combat (EC), tactical command and control countermeasures (C2CM), and Combat ID to the C3I Secretariat.

The organizational recommendations related to the CIO staff office presented in this Blueprint were developed to enable the Department to conduct a linked process of customer-focused value chain analysis and oversight. This will enable the Department to formulate policy guidance, develop long-range plans, monitor and evaluate program performance in the context of added value and to recommend the allocation of resources among the programs and components of the Department that will most directly lead to information superiority.

As a first step, the decision to conduct OSD-level oversight of information systems should not be triggered by the particular dollar value of an information technology (IT)[5] acquisition. Rather, the intensity of oversight should be focused on the affect of a particular acquisition activity on the value chain, including a clear definition of the local functional benefit in economic terms. This end-to-end focus is particularly important to interoperability and information assurance where "the weakest link" can be the failure point for the overall value chain or functional process. This systems-of-systems view recognizes that one cannot accurately predict the performance of a system by examining the individual components of the system: The important factors are found in the interfaces and in the interactions between the components.

Currently, DoD 5000.2R defines a Major Automated Information System (MAIS) Acquisition Program as an AIS acquisition program that is (1) designated by ASD(C3I) as a MAIS, or (2) estimated to require program costs in any single year in excess of 30

[5] In this Blueprint whenever the term information technology or IT is used it means the definition from ITMRA Sec. 5002. Definitions. "(3) INFORMATION TECHNOLOGY.-(A) The term 'information technology', with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product."

million in fiscal year (FY) 1996 constant dollars, total program costs in excess of 120 million in FY 1996 constant dollars, or total life-cycle costs in excess of 360 million in FY 1996 constant dollars[6]. The first category can include programs without regard to the amount of investment but it does not provide a clear reason for such a designation.

Therefore, the DoD 5000.2R definition should be replaced with the definition found in OMB Circular A-130[7]: "The term 'major information system' means an information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources."

For instance, a small-dollar program that creates large interoperability or information assurance problems clearly is important to the mission of the Department of Defense and should receive OSD-level attention.

The DRI noted that the Quadrennial Defense Review included as a central element of the Nation's defense strategy to "*Prepare* now for an uncertain future through a focused modernization effort, development of new operational concepts and organizations to fully exploit new technologies, and efforts to hedge against threats that are unlikely but which have disproportionate security implications – such as the emergence of a regional great power before 2015."

The challenges in preparing the information activities of the Department of Defense (DoD) for the changes called out in the QDR and DRI are spelled out in Joint Vision 2010. In Joint Vision 2010, the Chairman of the Joint Chiefs of Staff outlined the future direction of the military forces of the United States based on the emerging operational doctrines of Dominant Maneuver, Precision Engagement, Focused Logistics, and Full-Dimension Protection.

The execution of these operational doctrines, Joint Vision 2010 notes, depends upon information. "Sustaining the responsive, high quality data processing and information needed for joint military operations will require more than just an edge over an adversary. We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."

Joint Vision 2010 also warns, "There should be no misunderstanding that our effort to achieve and maintain information superiority will also invite resourceful enemy attacks on our information systems. Defensive information warfare to protect our ability to conduct information operations will be one of our biggest challenges in the period ahead. Traditional defensive IW operations include physical security measures and encryption. Nontraditional actions will range from anti-virus protection to innovative methods of

---

[6] DoD Regulation 5000.2-R, paragraph 1.3.2.

[7] OMB Circular A-130, Management of Federal Information Resources, Revised (Transmittal Memorandum No. 3), February 8, 1996, provides uniform government-wide information resources management policies as required by the Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35. Appendix III, "Security of Federal Automated Information Systems," provides a sound baseline for information assurance activities of the DoD.

secure data transmission. In addition, increased strategic level programs will be required in this critical area."[8]

The achievement of Information Superiority, then, is the appropriate goal around which to structure the offices supporting the ASD(C3I) and the CIO, DoD. More importantly, *the achievement of Information Superiority is the correct metric by which each decision concerning the information activities of the Department should be measured.* If a proposed action advances the Department towards the goal of Information Superiority it should be supported. If a proposed action does not advance the Department towards that goal, or worse moves away from that goal, then it should be resisted.

Today, the Department's information systems and activities would not meet any reasonable test of information superiority. Internal and external observers of the Department's information systems and activities note obsolescent and duplicative systems, excessive support costs, continued problems with interoperability, demonstrated serious shortfalls in information security[9], and an under-skilled information workforce.

Fundamental changes in the processes used for the management and oversight of the acquisition and operation of information technology is needed in order to achieve Information Superiority. To do otherwise, to keep doing what we have been doing, means that we will continue to get more of what we already have: high infrastructure costs and low utility.

Recommendation #5
The Secretary of Defense, consistent with his authority under ITMRA Sections 5122 and to support the objectives set out in Joint Vision 2010, direct that the oversight afforded the acquisition and use of information technology be based on the importance of the proposed acquisition of activity to achieving information superiority.

USE VALUE CHAIN ANALYSIS TO MEET THE DEPARTMENT'S GOALS

In the past the focus of oversight has largely been on the justification and acquisition of individual information systems. The degree of oversight was conditioned by the dollar value of each particular acquisition with little attention to the cumulative affect of these acquisitions on the overall capability of the Department or the aggregate gain to national security.

The business world has painfully leaned that a focus on individual information activities, within individual business units, will not assure a competitive position. To improve competitiveness, many companies have adopted a "value chain" or "supply chain" viewpoint. This means each of the activities used in creating value – up stream to exterior suppliers, internal to the company, and down stream to the end customer – are examined

---

[8] *Joint Vision 2010*, July 1996, page 16. The concepts put forth in Joint Vision 2010 are expanded in the *Concept for Future Joint Operations: Expanding Joint Vision 2010*, May 1997. The strategic, operational and tactical importance of Information Superiority is presented in Chapter 5 of this document.

[9] The Defense Science Board 1997 Summer Study Task Force on DoD Responses to Transnational Threats, October 1997, repeats the call for action to mitigate the Information Warfare threat made over the past four years by other DSB Task Force reports.

in the context of the overall value chain to reduce costs and improve responsiveness to the customer. Customer focus – the delivery end of the value chain – is the correct starting point for value-chain analysis.

A widely reported value chain example is Chrysler Corporation's Supplier Cost Reduction Effort (SCORE) which began in 1989 and has already reduced operating costs by over a billion dollars a year. With the addition of electronic commerce in 1997 Chrysler expects to increase its saving by over $2B per year by the year 2000. It is important to note that these savings did not result from the large-scale application of advanced technology. Rather, by getting all the information about particular value chains in one place and having all the involved parties look at the business processes and information flows they were able to identify waste and inefficiency and to look for a "solution supported by technology and not a technology providing a solution".[10] Through this process many small improvements were identified that together resulted in a large aggregate savings. A key factor in Chrysler's success was that it did not attempt to reap internal savings at the expense of others in the value chain.

In another example, the vice president of re-engineering at VF Services Inc., the world's largest publicly held apparel company, claims that "The only way to react quickly and increase profitability is to squeeze time out of the supply chain." "You have to sit down together and examine not only profitability goals and inventory levels but also how you can tie systems and communications together. It's very tough and requires a high level of trust and commitment."[11]

The Department has established Dominant Maneuver, Precision Engagement, Focused Logistics, and Full-Dimension Protection as its goals. Achieving the information superiority required to attain these goals can best be realized by linking these goals to the aggregate performance of specific functional processes, conduct "value chain" analysis to identify opportunities for improvement, including understanding how the underlying systems and communications are tied together to support these processes.

Recommendation #6

The Secretary of Defense, consistent with his authority under ITMRA Sections 5122, direct a shift in the oversight process for information technology (IT) from determining compliance with the processes used to acquire individual IT systems to an examination of the benefit(s) to the value chain of major functional activities that can be achieved through process improvement and the acquisition and effective use of information technology. The term value chain means the complete end-to-end linkage of functional process and information flows, including the supporting information technologies, that result in the delivery of goods and services.

VALUE CHAIN ANALYSIS AND REVIEWS

Value chain analysis, expanded upon below, is the appropriate approach to validation and oversight of evolutionary modifications to automated information systems which support linked functional processes.

---

[10] *CommunicationsWeek*, April 28, 1997 n660 p1, Chrysler saves big online.

[11] *CommunicationsWeek*, June 16, 1997 n668 p86, Supply chains get better links.

Value chain analysis does not mean the procurement activities associated with individual system acquisitions should be ignored. Whenever a Defense component acquires information technology, regardless of program size, the principles of sound program management should be followed. However, the oversight of individual system acquisitions should be conducted at as low a level as appropriate, given the importance of the program to the achievement of information superiority. Time and resource wasting activities such as holding multiple up-echelon acquisition reviews should be ruthlessly suppressed.

Any Project or Program Manager worthy of the title should be able to immediately produce upon a request from a component CIO or the CIO, DoD, or official in his or her acquisition oversight structure, current documentation of an approved budget, validated requirement that are consistent with the provisions of policy and law, proof of compliance with Departmental architectural guidance, a sound risk management approach, and a program schedule structured with sufficient internal milestones to enable program tracking.

The CIO's of the Department of Defense and of the military departments should randomly inspect the documentation of projects and programs to ensure the acquisition policies of the Department are understood and being followed. However, long experience with the MAISRC structure has demonstrated that it is not productive to attempt to "inspect in" compliance through an elaborate structure of tiered component and OSD-level reviews that attempt to examine every program. Such efforts added significant delay and cost to programs but did not demonstrate any significant improvement to the management of risk.

At a value chain review, the principal staff assistant (PSA) with responsibility for the functional area, supported by functional personnel from the defense components, would describe the end-to-end value chain of the activity under review. The review should be organized around the flow of information (whether manual or automated). The PSA would explain where investments in information technology are planned and underway, provide a breakout of aggregate and individual program costs and the anticipated, quantifiable, benefits (performance measures) to the functional activity.

The Program Executive Officer(s) and Program/Project Manager(s) responsible for delivering the information technology used in the functional area should attend the review. They should be prepared to answer any questions on program performance for any information technology acquisitions underway to support the functional activity. They should put specific emphasis on proactively identifying barriers beyond their control that are or that have the potential to limit the delivery of the technology or quantifiable benefits anticipated by the functional activity.

A word of caution about these reviews is in order. The depiction of functional process and data flows should be at a fairly high level. An attempt to portray functional activities at the atomic level is bound to fail because of the sheer complexity of Department-wide activities. Those interested in "malicious compliance" will attempt to encumber the review process with excessive detail. Much of the documentation requirements of the GPRA can be satisfied at an aggregated level. Redundant pre-reviews within the defense

components or by the supporting staffs in OSD should be prohibited as a wasteful activity.

As pointed out in the Chrysler example presented earlier, the objective is getting all the information about particular value chains in one place and having all the involved parties look at the business processes and information flows in an atmosphere of trust and cooperation. The appropriate role for the CIO and staff during these reviews is that of a coach with the benefit of a broad view of the Department's information activities: They should not play the role of policeman or inquisitor.

An end-to-end analysis of information flow is the only way to achieve the "shooter-to-sensor" capability needed to ensure dominance on the battlefield. The choice of order – shooter to sensor – rather than the typical ordering of sensor to shooter is deliberate. *All analysis of architectures and data flows should start at the pointed end of the spear and work back up the value-chain to the sustaining base!* This ensures that the very real "last dirt mile" isn't neglected in the analysis, as is often the case when the architects of virtual information highways start their analysis from the Pentagon down.

This combat-focused view also holds for determining the interfaces and support requirements of the C4ISR nodes embedded in weapon systems. In business terms, customer focused analysis always provides better answers than supplier focused analysis.

Once opportunities for improvement are identified in a value chain review, whether in process or supporting information technology, then speed of execution should be the principal metric. "Time to market" in commerce and in defense determines competitive position.

An area of regulatory and legislative concern is the affect on information technology activities related to the "color of money" (meaning the budgetary aggregation into research and development, procurement, and operations and maintenance accounts and the further partitioning into program element categories by function). The partitioning of taxpayer dollars into turf-related funding categories significantly limits the ability of the head of the agency to "conduct an acquisition of information technology." For example, a program manger may know that a small increase in the cost of a program would build in a training capability and yield significant downstream savings in the training accounts. However, the color of money – procurement vice O&M – is a barrier to the training office transferring funds to the program office. Similar distortions occur across all the funding "stovepipes."

However, the general thrust of ITMRA is that the head of the agency, through the CIO, ensures an efficient use of information technology in conjunction with improved functional practices. The three elements of an activity that are subject to change are people, process, and technology. The correct balance of these three variables yields the lowest total cost of ownership. Even if a value chain review shows that significant savings could accrue as a result of a rapid change in a process, enabled through the application of information technology, this may not be possible if the funds available in the functional area are not the correct "color" or are in a different program "stovepipe."

The CIO, DoD, in conjunction with the CFO, is encouraged to explore with the Office of Management and Budget, and with the Congress if necessary, ways to ensure the flexibility in moving money between accounting categories in order to make rapid changes in the information technology of the Department and obtain efficiencies that are just "too hard" under current processes.

Recommendation #7
The CIO, DoD, in conjunction with the appropriate principal staff assistant(s), the CIOs of the military departments, and the J-4 and J-6 of the Joint Staff, hold periodic value chain reviews of the major functional areas of the Department to determine if the information activities of the Department are effective and efficient and are on a path to support the attainment of information superiority.

CORE COMPETENCIES

In order to obtain information superiority – which includes seamless interoperability and robust information assurance – then the policy and oversight process must ensure the promulgation of and adherence to unambiguous Department-wide information technology building codes and standards. Within DoD, the C4ISR Architecture Framework, Levels of Information Systems Interoperability (LISI) Reference Model, Joint Technical Architecture, DII COE Integration & Runtime Specifications, DII COE User Interface Specifications, and other specifications and reference models, are necessary elements in the effort to achieve the degree of interoperability needed for information superiority.

However, promulgating frameworks, standards and specifications is not sufficient. These building codes must be followed by all information technology activities of the defense components. This is not the current case. The Inspector General, DoD, and the General Accounting Office have cited management shortcomings in oversight and application of the Department's building codes.[12]

Because the flow of information to and from the point of the spear must extend seamlessly into a variety of support functions, the CIO, DoD, should accelerate the application of these building codes to all information technology activities of the Department, not just the C4ISR segment.[13] The data flows from the "shooters to the sensors" and from the combatant forces to the sustaining services should achieve the highest level of standards compliance as soon possible. (This will be a particular

---

[12] GAO report AIMD-98-5, October 20, 1997, Defense IRM: Poor Implementation of Management Controls Has Put Migration Strategy at Risk; and, Office of the Inspector General, DoD, Report No. 98-023, November 18, 1997, Implementation of the DoD Joint Technical Architecture.

[13] DoDD 4630.5, Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I Systems, November 12, 1992, is the current policy document for interoperability. This directive should be updated to make the policy requirement a department-wide requirement and include strong compliance "teeth." The team reviewed an undated draft reissuance of DoDD 4630.5 entitled "Information Interoperability." This draft falls well short of the mark as it includes undefined terms, contains numerous "escape clauses" and does not assign clear oversight responsibility to ensure compliance. This draft should be rejected and a new directive drafted by the CIO, using active voice so that responsibilities are clear. The redraft should incorporate the concepts contained in the attached C4ISA white paper entitled "An Outcome Based Interoperability Improvement Process for the DoD" and the interoperability reference model entitled "Levels of Information Systems Interoperability," developed by the C4ISA Architectures Directorate.

challenge for interfaces into intelligence systems not under the control of the Department.)

There should be absolute commitment by the leadership of the Department to achieving joint interoperability between the combatant forces and sustaining services. Lack of interoperability is directly related to fratricide and a loss of combat effectiveness on the battlefield. The current uncoordinated modernization of base/post/camp-level infrastructures by the military departments – although each department's approach is technically sound within its own domain – will translate into joint interoperability problems on future battlefields and directly detracts from the goal of achieving information superiority.

Information technology that is directly in the value chain of a core mission may require less attention. However, activities that cannot demonstrate that they add value to the Department's core missions probably should be eliminated. Scarce funds should not be used in an effort to make ancillary systems interoperable and resilient to attack.

The Department, of course, is a part of the larger Federal government. Therefore, representatives of the CIO, DoD, should be active participants in the interoperability working group of the Federal CIO Council in order to understand and influence government-wide interoperability activities that could be barriers to achieving information superiority.

Program control mechanisms have not been effective in achieving interoperability. For example, once an information technology acquisition program passed the initial milestone review it was largely on auto-pilot. If a subsequent review determined that the program was being developed inconsistent with Departmental policy then the ASD(C3I) was limited to asking the Comptroller to withhold program funds. Basically, this was a break-fix strategy of waiting till a program was off-track before there was management intervention. Further, it was a hard strategy to execute because of the sunk costs in both time and money.

A better strategy for achieving the goal of information superiority would be to require an explicit affirmation by the program manager – and the component acquisition executive if under that structure – that he or she understands and will faithfully execute the program consistent with Departmental information technology policies. If the program departs from the path to information superiority, accountability will be clear. Under ITMRA, the CIO is empowered to recommend to the head of the agency that the program be terminated or redirected. In other words rather than being limited to stopping a program in place, the CIO can now propose a program redirection, if warranted.

Recommendation #8

The CIO, DoD, issue instructions requiring the defense components to demonstrate full adherence to the Joint Technical Architecture, the DII COE specifications, if applicable, and the defined level of the Information Systems Interoperability Reference Model, suitable for the function being supported, as a necessary condition for the expenditure of any funds for the development or acquisition of any system or application that is to be used by or support the combatant forces.

BUDGET

The value chain analysis recommended earlier, cross program analysis of C4ISR systems, the architectural responsibilities of the CIO, and other oversight activities require funds. The current level of funding (including personnel, rent, travel, etc.) in OASD(C3I) is about $15M plus $6M in FFRDC "Green Stamps," the CISA transfer under the DRI moves $42M per year to OASD(C3I), and the DARO office, as restructured, has requested $16M per year in the POM, cut to $7M by Congress. This later amount is probably inadequate for all the activities contained in the recommendations made above.

The C4ISR office requires about $12M per year to conduct cross program analysis of C4ISR and space systems, coordinate budget developments, ensure adherence to standards in C4 ISR systems, and provide oversight of service airborne reconnaissance systems as intended by Congress. None of these funds should be expended to manage programs more appropriately conducted by the defense components.

An aggressive Information Operations oversight program, including OSD-level Red Team exercise play needed to determine the degree of information assurance the Department has obtained, should be funded at $10M per year. None of these funds should be used for studies and analysis of information operations techniques or procedures more appropriately undertaken by the defense components.

An aggressive Year 2000 oversight effort with a strong focus on contingency planning should be funded at $10M per year, for each of the next two years.

The value chain analysis, architectural efforts, and IT oversight activities of the CIO, DoD, should be accommodated within the level of funding currently available to OASD(C3I), about $57M per year plus about $6M in FFRDC funding. However, this will require significant redirection of funding by the ASD(C3I)/CIO as many of the ongoing projects within OASD(C3I) have a narrow focus rather than the cross-cutting, systems-of-systems, value chain analysis needed to obtain information superiority. Further, a portion of the CISA budget has been used to conduct operational architecture studies on behalf of the CINCs. Such studies should be accomplished with funds available to the CINCs and supporting military departments. Although these studies do not require large expenditures they are not an appropriate OSD function.

In aggregate, the combined budgets from DARO, C3I, CISA, and Space organizations would total about $93M per year. Although this is a large sum of money it must be considered in context. Currently, the direct C4ISR and IT expenditures of the Department total about $50B per year. Approximately $10B per year of this spent on IT that directly supports over $150B per year of functional activities. If, through the wise expenditure of these OSD funds, the Department aggressively undertakes value chain analysis, including contracted technical analytic support, it should be able to achieve "each year at least a 5 percent increase in the efficiency of the agency operations, by reason of improvements in information resources management by the agency."[14] This would translate into over $7B per year of operational costs which could shifted from the support "tail" into modernization of combat "teeth." This would be a reasonable ROI on the OSD funds.

[14] Clinger-Cohen Act of 1996, Section 5132. Sense of Congress.

Recommendation #9
The Secretary of Defense permit the ASD(C3I) and the CIO, DoD, to retain sufficient funds to enable aggressive oversight and assessment of the value chains of major functional activities, including intelligence, C4ISR systems and activities, Information Operations, and the acquisition and effective use of information technology to support these functional activities, improve the efficiency of functional operations, and measure the Department's progress towards the achievement of information superiority.

MAISRC

The Major Automated Information System Review Council was established over two decades ago to satisfy the policies and procedures that grew out of the Brooks Act and the delegation of authority over information resource management to the Departments senior information resource management official by the head of the General Services Administration. This Council is a relic of the days when it was believed that a special body was required to oversee the acquisition of large, expensive main frame computers. The examination of value chains, as recommended in the Blueprint, cannot be accomplished by an organizational structure and process established to examine the acquisition of individual systems. It should be eliminated.

Recommendation #10
The CIO, DoD, in coordination with the USD(A&T), eliminate the Major Automated Information System Review Council.

The oversight processes put in place to replace the MAISRC should be structured to handle four distinct classes of information technology: military-unique technology; major IT system acquisitions where a total system solution is being acquired (also known as grand design systems), functional software applications designed to run on an installed computing and communications base; and, a common information utility such as the Defense Information Systems Network (DISN) and the Defense Information Infrastructure Common Operating Environment (DII COE).

If a military department or defense agency intends to acquire military unique information-related equipment that will entail production of more than a limited number of copies, such as a tactical radio or tactical fire control system, then it is appropriate to apply to that procurement the oversight processes used for defense acquisition programs as spelled out in DoD Regulation 5000.2R.

The track record in industry and government makes it clear that the acquisition of major automated information systems is a very high-risk undertaking.[15] Large amounts of cash are tied up for a long period of time before there is a payoff – assuming the program is one of the few that even succeed. If a defense component intends to acquire a major automated information system, then it should have to present to the CIO, DoD, a full business case analysis that is fully compliant with every aspect of the Government

[15] Based on data from the Standish Group. Washington Technology [January 22, 1998, p28] reports that only 27% of U.S. client/server projects are completed on time and on budget, 33% are completed late, over budget and/or over with fewer features than originally specified, and 40% are cancelled before completion. See also The Squandered Computer, Paul A. Strassmann, The Information Economic Press, 1997.

Performance and Results Act of 1993, Federal Acquisition Streamlining Act of 1994, the Paperwork Reduction Act of 1995, OMB Circular A-130, and OMB Circular A-11, prior to entry into Milestone 0 of the DoD Regulation 5000.2R. In other words the bar for obtaining approval for a grand design approach should be set very high. If the business plan is approved than the major program oversight processes spelled out in DoD 5000.2R should be followed in detail.

The acquisition of functional software applications, if written to Application Program Interface specifications to run on an installed computing and communications base, should be justified through the value chain analysis, consistent with GPRA, as described earlier. Such software purchases, or software developments if done consistent with modular contracting as spelled out in ITMRA, should not require additional OSD-level oversight.

The acquisition of components for a common information utility such as the Defense Information Systems Network are addressed later in this report.

Recommendation #11
The USD(A&T), in coordination with the CIO, DoD, establish an Overarching Integrated Product Team, within the Defense Acquisition Board structure, to review C4ISR and information technology acquisitions that will lead to the production of multiple copies of military unique information technology or that involves the acquisition of a major automated information system, as so designated by the CIO, DoD.

PREPARE THE STAFF FOR THE 21ST CENTURY

The shift in oversight focus, outlined above, will require some very wrenching changes in organization, process, trust, and commitment. To conduct such a value chain oversight the Department will have to develop new analytic skills and the capability to portray system-of-system linkages, information flows, and process activities in the context of information technology architectures[16].

However, these skills are well worth mastering, as they will have very high payoff. These analytic skills and data sets can support, in an integrated manner, an examination of functional process improvements as required by the Government Performance and Results Act (GPRA)[17] and the Clinger-Cohen Act[18], the interfaces and interoperability

---

[16] See OMB Memorandum M-97-16, Information Technology Architectures, June 18, 1997 for a definition of architectures. This memorandum provides the policy context for complying with the Clinger-Cohen Act (Section 5125(b)(2)) which assigns the CIO the responsibility of "developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture." This memorandum provides a lucid discussion of the linkages between business process, information flows and relationships, applications, data, technology, technical reference models, standards, and security.

[17] The Government Performance and Results Act of 1993. The General Accounting Office documents, GAO/GGD-10.1.16, Agencies' Strategic Plans Under GPRS: Key Questions to Facilitate Congressional Review, May 1977; and GAO/AIMD-10.1.13, Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making, February 1997, provide an excellent stating place for designing the review process to be used for functional and supporting infrastructure reviews.

between systems, the affect – positive or negative – on the information assurance posture of the Department, the risks to business continuity by Year 2000 failures, and the specific requirements, costs and schedules of all associated acquisitions in a particular functional value chain.

Recommendations #12
The ASD(C3I) undertake an aggressive educational program to teach the concepts and processes of commercial value-chain analysis to the staffs supporting the ASD(C3I), the CIO, DoD, and the CIOs of the defense components.

TECHNICAL CHANGE MANAGEMENT

A factor complicating information and information technology policy development and oversight is the rate of change of technology. Moore's Law[19] continues to drive down the cost of computer hardware and the ongoing revolution in communications technology is driving a rapid shift from switched circuits (smart centers) to communications cells (smart ends) is fundamentally changing the economics of computing and communications.

These changes should be recognized in policies for the acquisition of technology to support functional processes. For example, because of the varied useful life of system components, total "systems" should rarely be acquired[20]. Rather, as business or functional practices change, software applications that encapsulate the new business rules and can access and manipulate data should be rapidly acquired and run on top of already existing infrastructures such as the Defense Information Infrastructure Common Operating Environment (DII COE).

Maintaining a clear separation of data, functional software applications, and the supporting technical infrastructure will enable the Department and defense components to make continuous technical refreshment in each area without the costs of scrapping total systems and starting over. This approach is consistent with the intent of the Congress that agencies give preference to the modular acquisition of information capabilities.[21]

---

[18] The Clinger-Cohen Act of 1996 (Public Law 104-106). Subdivision E of the Clinger-Cohen Act of 1996 was formally known as the Information Technology Management Reform Act of 1996. The acronym ITMRA is a common shorthand for this law.

[19] Moore's Law says that computing (microprocessor chip) capability per unit cost doubles every 18 months. Skeptics note that what Moore gives Gates takes. They caution that the growth in the size of desktop software applications (bloatware) continues to outpace the increase in desktop computing capacity. Because the costs of support increase with complexity, the combination of cheaper chips and larger software programs drives up training and support costs without a measurable gain in productivity for the end user.

[20] Functional software applications should be written to Application Program Interface specifications which "hide" the underlying computing technology. The enforced separation of applications, data, and supporting telecomputing services is a sound design approach and lessens the potential of the activity becoming captive to proprietary technology.

[21] Modular Contracting is defined in Section 35 of the Office of Federal Procurement Policy Act [Sec. 5202 of ITMRA] Congress. Section 35(a) says, "The head of an executive agency should, to the maximum extent practicable, use modular contracting for an acquisition of a major system of information technology." Modular contracting is the acquisition, in less than 18 months each, of interoperable increments where each increment comprises a system or solution does not depend upon any subsequent increment to perform its

The progress the Defense Information Systems Agency (DISA) has achieved in developing the Defense Information Infrastructure Common Operational Environment (DII COE) is a good example of the benefits that accrue from continuous, incremental improvement. At any point in time the DII COE contains numerous individual components of technology. Over the next decade all of the components currently used in the DII COE will be replaced yet the DII COE will still exist as an integrated information utility.

The DII COE example highlights the reality that a sound process of managing technical change is much more important than the purchase, at a specific point in time, of any specific component of information technology. It follows that in monitoring and evaluating program performance of information technology acquisitions, priority should be given to maintaining the long-term technical health of the Department over reaping a short-term gain.

In this context, functional activities would have the primarily responsibility for identifying changes, additions or replacements to existing hardware and software to improve business process. The justification for the expenditure of resources to support particular functional activities would be separated from the process used to evolve the Department's common information utility services. Thus, the continued evolution of the Department's information utility services, such as the DII COE, requires oversight independent of specific functional activities.

Oversight of common infrastructure investment is best conducted in the context of managing a technical portfolio. This requires an analytic capability to forecast technical purchase, deployment, sustainment, and retirement costs. Assessing these costs is much more complex than just adding up the price of system components. For example, the benefits of improving the security of networks accrues to many functional activities that use these networks but individually no specific functional user has the responsibility nor would he or she be willing to assume the costs of protecting the networks.

Thus, the justification and review of common services such as information assurance should be treated separately from that of specific functional activities. Likewise, just as the too-early introduction of technology can have high deployment and training costs, the retention of technology beyond its useful life can be very expensive and also limit operational capability across many functional areas. Again, the management of technology refreshment of common information utility services should be addressed by the Department from a common utility services perspective.

Defense-wide activities that should be afforded OSD-level portfolio management include Year 2000, the DII COE, Electronic Commerce/Electronic Data Interchange (EC/EI), directory/registry services (X.400/X.500), certificate authorities, and information assurance. The November 15, 1997, document, "A Management Process for a Defense-wide Information Assurance Program (DIAP)" is a reasonable model for establishing portfolio management of defense-wide infrastructure services.

---

principal functions. In a nutshell: Do not buy large, complex systems. Rather, it is smarter to buy continuous improvement through the lower risk acquisition of small increments.

Technical portfolio management requires solid economic analysis and identification of department-wide costs and benefits. However, the economic analysis of information utility services appears to be a weakness in the Department. Recent reports indicate that the commingling of appropriated and revolving funds in the development of such utility services may be a contributing factor.

When proposed enhancements to common utilities for the "common good" are primarily justified on the benefit to a specific functional activity then they are not funded. Individual activities do not want to pay for the benefit of others. Improvements to the Department's information technology infrastructure "for the common good" should be afforded policy guidance, oversight and funding separate from that afforded specific functional activities.

To that end, the CIO of the Department should develop the analytic capabilities necessary to separately identify the steps and associated costs required for ensuring the robust information utility services needed to obtain information superiority and the steps and costs needed for ensuring discrete functional activities can optimize their information-related activities.

Recommendation #13
The CIO, DoD, issue instructions to the Defense Information Systems Agency and the Chief Information Officers of the military departments to justify proposed technical changes to the DII COE, Defense Megacenters, EC/EDI, Directory Services, Information Assurance, and service-unique infrastructure systems, with an economic analysis that is independent of the economic benefits that accrue to specific functional activities.

DEPARTMENT-WIDE INFORMATION ACTIVITIES

The Defense Information Systems Agency (DISA) plays a central role in the execution of department-wide information technology activities. The other defense components also play an important role in the acquisition and fielding of the Department's information technology infrastructure. The integration and interoperability of the multiple information activities acquired by the various defense components remains a challenge to the attainment of information superiority.

The CIO, DoD, and supporting staff, must rely upon DISA for timely and accurate technical and architectural information concerning both defense-wide functions for which DISA is responsible and the interfaces between defense-wide and component information activities.

The importance of clear lines of communication between internal DISA offices and the ASD(C3I) and CIO staffs performing C4ISR Systems and information technology oversight responsibilities is clear. However, the team found that the lines of communications between DISA offices and OSD have deteriorated to the point where they will not adequately support end-to-end value chain analysis.

Simplification of organizational structures and clear assignment of responsibilities for internal and external communications should be a high priority.

Recommendation #14

The CIO, DoD, issue instructions requiring the defense components to develop the capability to provide cost and operational information associated with communications networks, data processing activities, and data flows as is necessary to support the architecture, value chain analysis, and oversight activities of the CIO, to include oversight of customer satisfaction.

SIMPLIFY, SIMPLIFY, SIMPLIFY

The team found numerous policy memorandum, guides, and draft procedures, in OSD and in the defense components, that both pre-date and post-date ITMRA, that are either inconsistent with ITMRA requirements or are too-narrowly drafted. In several instances sound policies are limited to C4ISR systems when they should apply to information technology across the department[22].

---

[22] An incomplete, annotated, listing in no particular order of such documents follows: USD(A&T)/ASD(C3I) memorandum, Implementation of the DoD Joint Technical Architecture, August 22, 1996 [Should be extend to IT department-wide]; ASD(C3I) memorandum, Establishment of a Defense Information Infrastructure (DII) Common Operating Environment (COE) Configuration Management Structure, April 29, 1997 [Overlaps other policy memoranda]; ASD(C3I) memorandum, Global Command and Control System (GCCS) Oversight, August 31, 1993 [Oversight inconsistent with ITMRA]; ASD(C3I) memorandum, Management and Life-Cycle Support for the Global Command and Control System, June 26, 1995 [Appears to be inconsistent with later policy memoranda]; USD(A&T)/ASD(C3I)/J-6 Joint Staff memorandum, DoD Architecture Coordination Council (ACC), January 14, 1997 [Relationship to CIO, Council unclear]; Draft USD(A&T)/ASD(C3I) memorandum, Transfer of Major Automated Information System Review Council (MAISRC) Functions to the Defense Acquisition Board (DAB) [New name, retains flawed system focus rather than an information superiority view]; ASD(C3I) memorandum, Information Technology (IT) Investment Management Insight Policy for Acquisition, July 25, 1997 [Guidance based on dollar thresholds, not importance to DoD]; Draft reissuance of DoD Directive 8000.1 [Use of passive voice makes accountability difficult, contains modifiers inconsistent with ITMRA, contains definitions inconsistent with OMB Circular A-130 and drops the sound principles of information management contained in enclosure 3 of the current directive that are consistent with and add value to ITMRA]; draft Directive 4630.5, Information Interoperability [Includes undefined terms, contains numerous "escape clauses" and does not assign clear oversight responsibility to ensure compliance]; draft revision to DoD 5000.2R [IT Guidance based on dollar thresholds, not importance to DoD]; ASD(C3I) memorandum, Guide For Managing Information Technology (IT) as an Investment and Measuring Performance, Version 1.0," February 14, 1997 [The attached very voluminous guide of the same name, dated March 3, 1997, may be a useful academic tutorial but in reality this guide is a particularly egregious example of over-regulation that focuses on the tree leaves, rather than on the forest. If this guide were to actually be followed by the defense components it would cost the Department tens of millions of dollars annually with little improvement in management: A top candidate for cancellation. In contrast, the Air Force CIO has issued an "Air Force Information Technology Investment Performance Guide," August 1997, that is concise and uses clear language. A good model for OSD issuance's.]; ASD(C3I), memorandum DoD CIO Business Plan, July 8, 1997 and attached document, DoD Chief Information Officer Business Plan, Version 1, May 1997 [Descriptive, passive voice avoids accountability, does not constrain and guide activities as a meaningful plan would do.]; and, ASD(C3I) memorandum Information Technology Management (ITM) Strategic Plan, March 20, 1997, and attached document Information Technology Management (ITM) Supporting National Defense (ITM Strategic Plan), Version 1.0, March 1997 [Terminology inconsistent with other IT policy memoranda]. A striking example of the type of unnecessary oversight committee that should be eliminated is the JSMB. This Board is made up of 24 senior officials, three ex officio members, and two executive secretaries. Such a body cannot provide either the crisp decisions or the focused oversight required to achieve information superiority.

On a positive note the team did find a consistent set of policy documents from the Office of Management and Budget that implement ITMRA and GPRA and a very clear memorandum by the Secretary of Defense outlining the responsibilities of the CIO, DoD[23].

It appears that various OSD offices independently promulgated overlapping and inconsistent guidance for information technology and information resource management. The lack of strong leadership and clear DoD IT policy that is consistent with ITMRA and OMB policy documents "can still derail the Department's best efforts to reform its business practices."[24]

The Department would be well served by stopping the practice of crafting parochial policy documents and guides and, wherever possible, to use existing Federal-level policy documents and guides to avoid the cost of generating duplicative guidance documents. For instance, the Department should use OMB Circular A-130, Management of Federal Information Resources, as its basic policy guide for information technology. The GAO document GAO/AIMD-10.1.13, "Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-Making," dated February 1997, is an excellent guide for both program self-assessment and for the oversight of investments in information technology. The CIO Council Committee on Capital Planning and IT Investment has published a very good guide entitled "Information Technology Investment: 'First Practices'," dated February 28, 1997.

In addition to duplicative policy documents and guides, the Blueprint Team observed that a large number of committees and boards of questionable value have been established over the years for the coordination and oversight of intelligence, security, C4ISR systems, and information technology. Many of these committees and boards confuse the lines of authority and diffuse accountability. Consistent with the principle of good management and the guidance outlined in Deputy Secretary of Defense memorandum, "Department of Defense Reform Initiative Directive #8 – Reducing the Number of Committees," December 10, 1997, the majority of these committees and boards should be eliminated.

Recommendation #15

The ASD(C3I) (consistent with delegations of authority), in the next 90 days: 1) conduct a through review of existing and proposed directives, instructions, policy memoranda, guides, frameworks, standards, charters of committees, boards and working groups, and other materials related to C4ISR and information technology; 2) expeditiously cancel, withdraw, or request the cancellation of unnecessary policy and guidance memoranda, instructions, guides, and other material; 3) issue clear, consistent instructions for the acquisition of C4ISR systems and the use of information technology; and, 4) strongly discourage supplementation of OSD policy and instructions by the defense components.

---

[23] Secretary of Defense memorandum, "Implementation of Subdivision E of the Clinger-Cohen Act of 1996 (Public Law 104-106)," June 2, 1997.

[24] USD(C) memorandum, "FY 1999 Passback to Department of Defense," December 12, 1997

Additional Recommended Actions

Deputy Secretary of Defense memorandum, 'Establishment of the Deputy Under Secretary of Defense for Space Acquisition and Technology Programs," dated December 10, 1994.

Cancel. Consistent with the recommendations of the Defense Reform Initiative (DRI) and Deputy Secretary of Defense memorandum, "Department of Defense Reform Initiative #11 – Reorganization of DoD Space Management Responsibilities," dated December 19, 1997, the Commander in Chief, U.S. Space Command and the Director, National Reconnaissance are preparing a coordinated proposal on the realignment of the non-policy space functions of the DUSD(Space). The Blueprint Team recommends OSD-level non-policy functions be realigned to a Space and Navigation Directorate under the C3 Secretariat.

Joint Space Management Board (JSMB).

Eliminate. This board is made up of 24 senior officials, three ex officio members, and two executive secretaries: such a body cannot efficiently provide integrated program planning, efficient resource allocation, or accountable management for the nation's national security space program.

Secretary of Defense Memorandum, "Defense Intelligence Programs," dated June 26, 1995.

Cancel. This memorandum is the basis for the Expanded Defense Resources Board EDRB) co-chaired by the DCI and Deputy Secretary to review all Defense intelligence resources. This is supported by an Intelligence Program Review Group co-chaired by the Executive Director, Intelligence Community and the ASD(C3I) to examine major issues and alternatives between the National Foreign Intelligence Program (NFIP), Joint Military Intelligence Program (JMIP) and the Tactical Intelligence and Related Activities (TIARA). These bodies have not yielded benefits commensurate with the excessive time and manpower they consume.

Create an Intelligence Program Coordinating Group that would meet monthly to coordinate NFIP, JMIP and TIARA budget activities. The Director, Community Management Staff and the ASD(C3I) would hold quarterly status reviews to assess any open issues. Those major issues that could not be resolved within the Department or Intelligence Community, based on mutual review, would be forwarded within channels to the DCI and Deputy Secretary for discussion at a June meeting in time to influence budget decisions. The Deputy Secretary, after receiving the DCI's advice, would provide appropriate budget direction to the Defense components.

Regular coordination meetings throughout the year, coupled with a greatly simplified process to surface issues, should result in improved coordination between the DCI and Defense at much less cost.

Deputy Secretary of Defense memoranda, Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement, dated October 13, 1993, and

"Management Structure for the Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement, April 6, 1994.

Cancel. The Government Performance and Results Act of 1993 and the Information Technology Management Act of 1996 have overtaken this guidance. System migration has a role in modernizing the Department's infrastructure and lowering support costs. However, migration guidance established in 1993 may no longer be consistent the Department's Strategic IT Plan (required by GPRA after September 1997). IT investments should only be undertaken if supported by a quantifiable functional benefit accompanied with an improvement in information superiority.

The functions of the Enterprise Integration Executive Board and Corporate Management Council set out the in the April 1994 memorandum, cited above, are now more appropriately within the scope of the CIO Council.

USD(A&T)/ASD(C3I) memorandum, Implementation of the DoD Joint Technical Architecture, August 22, 1996

Cancel. CIO rewrite new policy instruction and extend the JTA Version 2.0 to IT department-wide.

ASD(C3I) memorandum, Establishment of a Defense Information Infrastructure (DII) Common Operating Environment (COE) Configuration Management Structure, April 29, 1997

Cancel. Overlaps other policy memoranda. If needed, CIO rewrite and reissue.

ASD(C3I) memorandum, Global Command and Control System (GCCS) Oversight, August 31, 1993

Cancel. Oversight inconsistent with ITMRA and recommendations in this report.

ASD(C3I) memorandum, Management and Life-Cycle Support for the Global Command and Control System, June 26, 1995

Cancel. If needed, reissue consistent with ITMRA and recommendations in this report.

USD(A&T)/ASD(C3I)/J-6 Joint Staff memorandum, DoD Architecture Coordination Council (ACC), January 14, 1997

Cancel. DoD Architecture Coordination Council overlaps function of the CIO, Council.

Draft USD(A&T)/ASD(C3I) memorandum, Transfer of Major Automated Information System Review Council (MAISRC) Functions to the Defense Acquisition Board (DAB)

Do not approve as drafted. Contains flawed system focus rather than a focus on obtaining information superiority. The CIO should issue a policy memorandum canceling MAISRC outright.

ASD(C3I) memorandum, Information Technology (IT) Investment Management Insight Policy for Acquisition, July 25, 1997

Cancel. Guidance based on dollar thresholds, not importance to DoD.

Draft reissuance of DoD Directive 8000.1

Do not approve as drafted. Use of passive voice makes accountability difficult, contains modifiers inconsistent with ITMRA, contains definitions inconsistent with OMB Circular A-130 and drops the sound principles of information management contained in enclosure 3 of the current directive that are consistent with and add value to ITMRA. The CIO, DoD, redraft consistent with the recommendations contained in this report.

Draft Directive 4630.5, Information Interoperability

Do not approve. Includes undefined terms, contains numerous "escape clauses" and does not assign clear oversight responsibility to ensure compliance. The CIO, DoD, redraft to make accountability for interoperability and process for verification clear.

Revision to DoD 5000.2R

CIO, DoD, should rewrite those sections that relate IT Guidance (MAIS) to dollar thresholds, rather than the importance to DoD and Information Superiority. Use the definition of major system contained in OMB Circular A-130

ASD(C3I) memorandum, Guide For Managing Information Technology (IT) as an Investment and Measuring Performance, Version 1.0," February 14, 1997 and guide of the same name, dated March 3, 1997,

Cancel. Requires excessive documentation and is inconsistent with the other Federal and DoD policy documents. Use the "Air Force Information Technology Investment Performance Guide," August 1997 as a model for OSD issuance of a new investment guide, if needed.

ASD(C3I), memorandum DoD CIO Business Plan, July 8, 1997 and attached document, DoD Chief Information Officer Business Plan, Version 1, May 1997

Cancel. Contains descriptive, passive voice that avoids accountability, and does not constrain and guide activities as required in a meaningful plan.

ASD(C3I) memorandum Information Technology Management (ITM) Strategic Plan, March 20, 1997, and attached document Information Technology Management (ITM) Supporting National Defense (ITM Strategic Plan), Version 1.0, March 1997

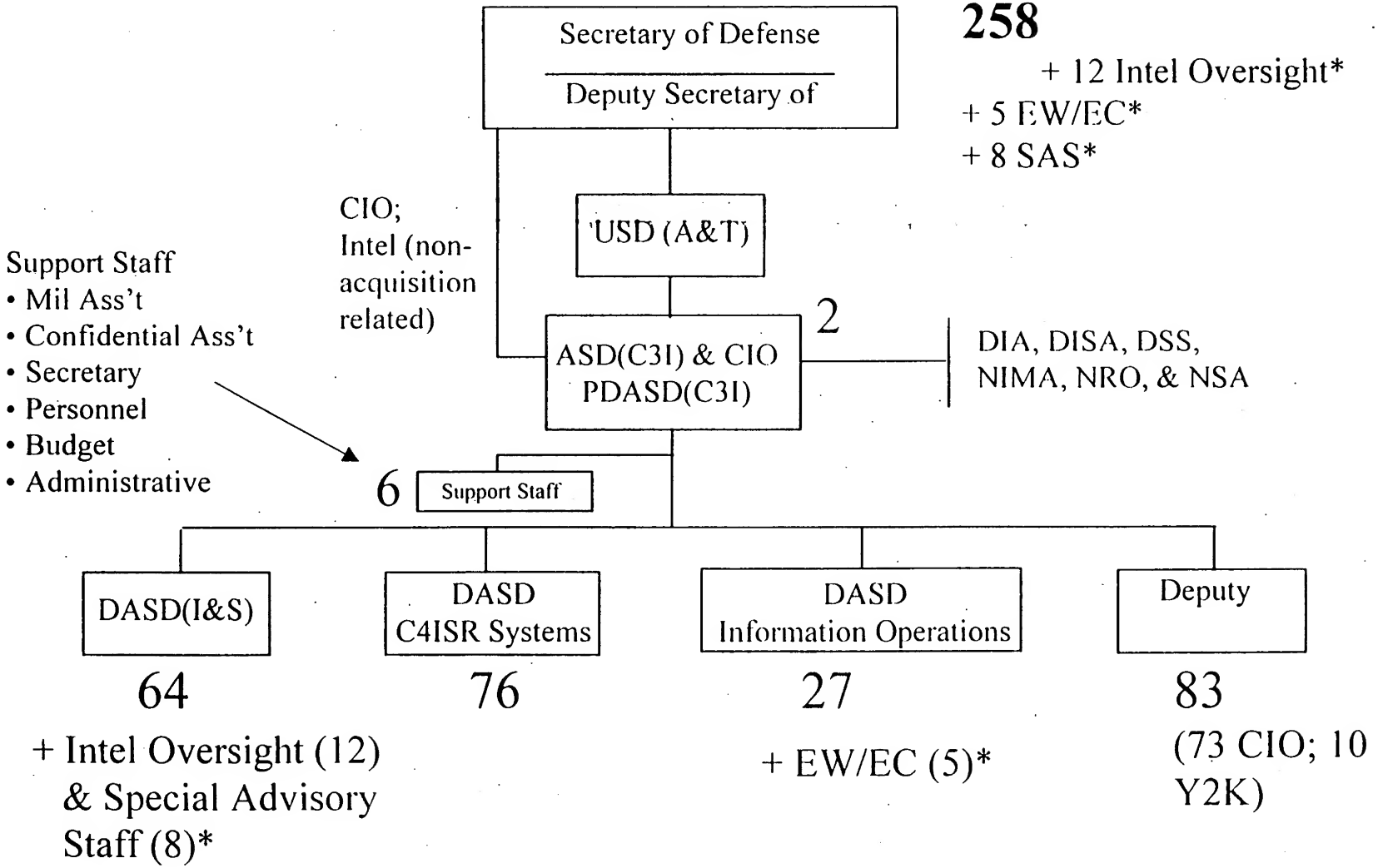
Cancel. Terminology is inconsistent with other Federal and Departmental IT policy memoranda

Attachment

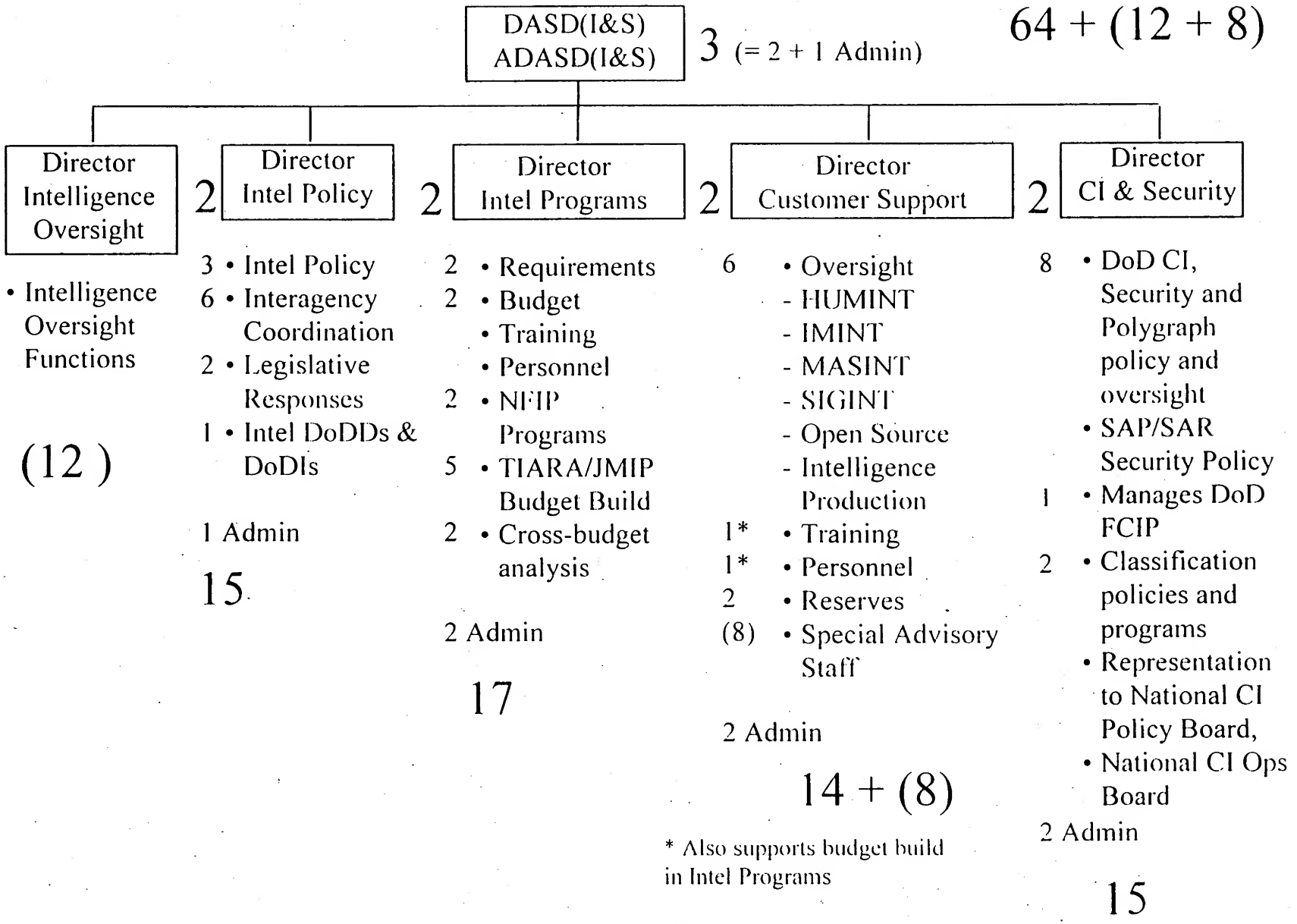
Baseline ASD(C3I) Organization

CIO Staff Functions

Interoperability White Paper



*Recommended

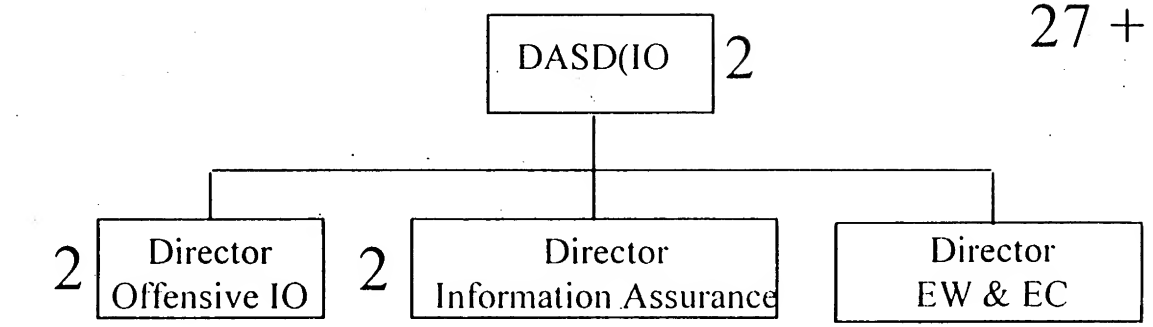

DASD(I&S)
ADASD(I&S)
3 (= 2 + 1 Admin)
64 + (12 + 8)
Director Intelligence Oversight
• Intelligence Oversight Functions
(12)
2
Director Intel Policy
3 • Intel Policy
6 • Interagency Coordination
2 • Legislative Responses
1 • Intel DoDDs & DoDIs
1 Admin
15
2
Director Intel Programs
2 • Requirements
2 • Budget
• Training
• Personnel
2 • NFIP Programs
5 • TIARA/JMIP Budget Build
2 • Cross-budget analysis
2 Admin
17
2
Director Customer Support
6 • Oversight
- HUMINT
- IMINT
- MASINT
- SIGINT
- Open Source
- Intelligence Production
1* • Training
1* • Personnel
2 • Reserves
(8) • Special Advisory Staff
2 Admin
14 + (8)
* Also supports budget build in Intel Programs
2
Director CI & Security
8 • DoD CI, Security and Polygraph policy and oversight
• SAP/SAR Security Policy
1 • Manages DoD FCIP
2 • Classification policies and programs
• Representation to National CI Policy Board,
• National CI Ops Board
2 Admin
15

7

DASD C4ISR — 2

Director C4 — 2	Director ISR — 2	Director Space & Navigation — 2	C4ISR Integration — 2
3 • C4 Systems	20* • ISR Systems	4 • Space Architectures	4 • C4ISR Systems Cross-Program Integration
3 • Communications	1 • I&W & TW/AA Sys.	• Space Systems	2 • C4ISR Resources & PPBS Coordination
- Terrestrial	2 • ISR Trade-offs	1 • Environmental Sensing	1 • FFRDC Oversight
- Space	- Air	1 • Launch	- MITRE/SEI
- Special Purpose	- Space (Gov't)	3 • Navigation Systems	1 • C4ISR Program Acquisition Coordination
1 Networks	- Space (Comm.)	• Safety Programs	1 • DAB
1 • Messaging	- Unattended Ground-based	1 • FAA Coordination	
• NCS Oversight	- TW/AA	1 • Combat ID	1 Admin
• NCA/Continuity	4 • Special Projects		
3 of Operations	3 Admin	2 Admin	
• Allied & Coalition C4 Coordination	(*20 from DARO)		
2 Admin			
1	3	1	1

27 + (5)



12
- IO Policy
- IO Centralized Planning & Coordination
- Preparation of the IO Battlefield
- IO Security Guidance
- Oversight DoD-level Red Team & IO Exercise Evaluation

2 Admin

16

1
- IA Policy

3
- IA Centralized Planning & Coordination with CIO I&I

1
- Defense-wide Information Assurance Program

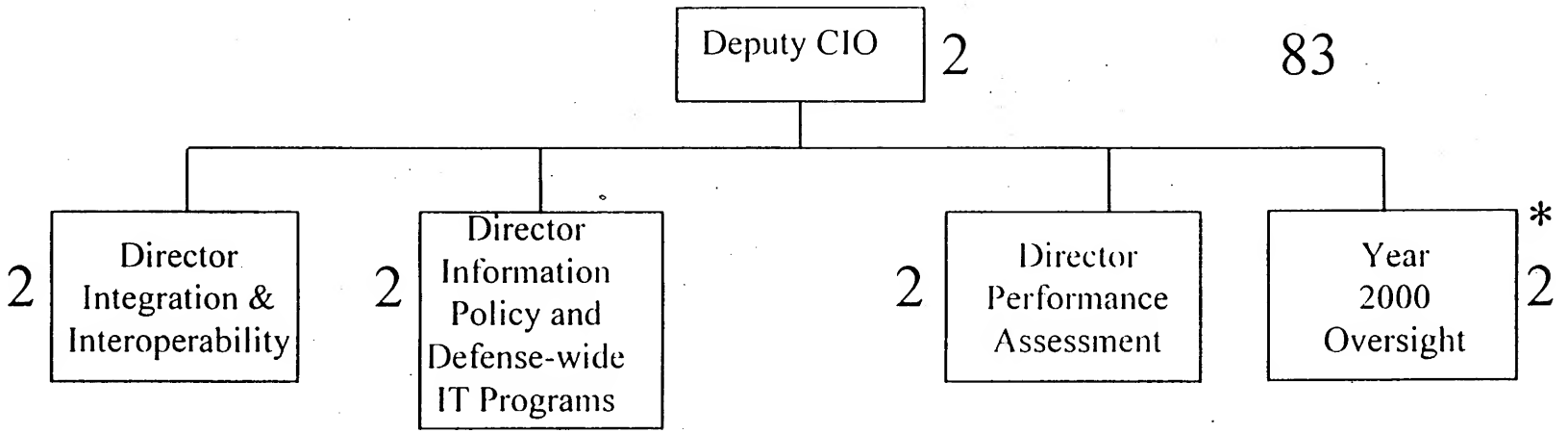
1
- Information Infrastructure Protection

1 Admin

9

- EW Systems
- EC Systems

(5)



6 • Architectures
2 • Standards
10 • DSC
3 • Interface & data analysis
4 • DII Baseline
2 • Next-generation Architecture & DII
1 Graphics Support
3 Admin

37

5 • IM Policies
- Benefit & Risk Analysis
- Process Improvement
- Best Practices
- Investment criteria
- Interagency representation

1 • Strategic Plan
1 • IT/PPBS Coordination with CFO
1 • Ex. Sec & Support to CIO Council
1 • Congressional matters
2 • Training
1 • EC/EDI
1 • Certificate Authorities & Directory Services
• Multi-agency Acquisitions
2 • Spectrum Policy and Oversight
1 • Encryption Policy
3 Admin

21

6 • Performance & Results-based Outcome Assessments
2 • Benchmark
1 • Annual Report
1 • 43 Exhibits
1 Admin

13

5 • Year 2000 Oversight
3 • Year 2000 Contingency Planning

10

*Sunset 10/30/2001

CIO

Promotes improvements to DoD work processes and supportive information resources.

Provides management and oversight of all DoD information technology and national security systems.

Is the primary DoD representative of the Department to Federal and interagency bodies supporting Federal information technology policies.

Designs and implements a process for maximizing the value and assessing and managing the risks of DoD information technology acquisitions, in coordination with the DoD Planning, Programming and Budgeting System (PPBS) authorities and acquisition authorities, and in accordance with Section 5122 of the ITMRA.

Institutionalizes performance-based and results-based management for information technology in coordination with the Chief Financial Officer of the Department of Defense, the OSD Principal Staff Assistants and the Don Components.

Issues DoD Instructions, DoD publications and one-time directive-type memoranda

Ensures that the information security policies, procedures, and practices of the Department of Defense are adequate.

Oversees contracts that provide for multi-agency acquisitions of information technology in accordance with Section 5124 of the ITMRA and guidance issued by the Director of the Office of Management and Budget.

Provides advice and other assistance to the Secretary of Defense and other senior management personnel of the Department to ensure that information technology is acquired and information resources are managed for the Department in a manner that implements the policies and procedures of the ITMRA, consistent with Chapter 35 of Title 44, United Staten Code, and the priorities established by the Secretary of Defense.

Develops, maintains, and facilitates the implementation of a sound and integrated information technology architecture for the Department of Defense in accordance with the requirements of Section 5125(b)(2) of the ITMRA.

Promotes the effective and efficient design and operation of all major information resources management processes for the Department of Defense, including improvements to work processes of the Department of Defense in accordance with Section 5125(b)(3) of the ITMRA.

Monitors the performance of IT programs of the Department of Defense, evaluates the performance of those programs on the basis of applicable performance measurements, and advises the Secretary of Defense regarding whether to continue, modify, or terminate a program or project in accordance with Section 5125(c) (2) of the ITMRA.

Establishes and implements training initiatives, in coordination with the Under Secretary of Defense for Personnel and Readiness, to ensure the requirements of Section 5215(c)(3) of the ITMRA are met.

Reports to the Secretary of Defense on the progress made in improving the Departments information resources management capability.

Establishes policies and procedures, in consultation with the Chief Financial Officer of the Department of Defense, to:

1. Ensure that accounting, financial, and asset management systems and other information systems of the Department of Defense are designed, developed, maintained, and used effectively to provide financial or program performance data for financial statements of the Department of Defense;
2. Ensure that financial and related performance data are provided on a reliable, consistent, and timely basis to DoD financial management systems; and
3. Ensure that financial statements support assessments and revisions of mission-related processes and administrative processes of the Department of Defense and performance measurement of investments made by the Department of Defense in information systems.

Identifies any major information technology acquisition program, or any phase or increment of such a program, that has significantly deviated from the cost, performance, or schedule goals established for the program in the strategic information resources management plan.

Develops a departmental strategic plan that addresses the management and use of IT capabilities.

Calls and chairs the CIO Council of the Department of Defense

Director of Integration and Interoperability

In support of the CIO, DoD:

Provides for the development, maintenance, and facilitates the implementation of a sound and integrated information technology architecture for the Department of Defense in accordance with the requirements of Section 5125(b)(2) of the ITMRA.

Coordinates standards, frameworks, and guides for the development and analysis of the integrated and interoperable flow of information

Promotes the effective and efficient design and operation of all major information resources management processes for the DoD, including improvements to work processes of the DoD IAW Section 5125(b)(3) of the ITMRA, through the application of analytic skills and tools in order to illuminate the interfaces and flows of information across major functional processes of the Department.

Maintains, with the support of the Defense Information Systems Agency and the other Defense components, the baseline of the Defense Information Infrastructure

Provides analytic support to the definition of the next-generation architecture and technical growth path for the DII

Director of Information Policy and Defense-wide IT Programs

In support of the CIO, DoD:

Develops policies that result in processes for maximizing the value and assessing and managing the risks of DoD information technology acquisitions, in coordination with DoD Planning, Programming and Budgeting System (PPBS) authorities and acquisition authorities, and in accordance with Section 5122 of the ITMRA.

Prepares DoD Instructions, DoD publications and one-time directive-type memoranda.

Serves as the Executive Secretary of the CIO Council, calls meetings at the direction of the CIO, prepare the agenda and other meeting materials and provide administrative support as needed, and maintain records of Council decisions and assigned actions in a data base that is accessible by Council members.

Provides support to the CIO, DoD in meetings of Federal and interagency bodies supporting Federal information technology policies, including coordination of congressional actions concerning the functions of the CIO.

Establishes and implements training initiatives and assessments, in coordination with the Under Secretary of Defense for Personnel and Readiness, to ensure requirements of Section 5215(c)(3) of the ITMRA are met.

Provides oversight of the Information Resources Management College of the National Defense University in its role as the primary training source to met the ITMRA training needs of DoD CIOs. executives, and senior-level managers.

Designs, implements, and maintains a process for maximizing the value and managing the risks of DoD information technology acquisitions, in coordination with DoD Planning, Programming and Budgeting System (PPBS) authorities and acquisition authorities, and in accordance with Section 5122 of the ITMRA that:

1. Provides for the selection of information technology investments to be made by the Department,
2. Is integrated with the processes for making budget, financial, and program management decisions within the Department;
3. Includes minimum criteria to be applied in considering whether to undertake a particular investment in information systems, including criteria related to the quantitatively expressed projected net, rink-adjusted return on investment and specific quantitative and qualitative criteria for comparing and prioritizing alternative information system investment project.
4. Provides for identifying information systems Investments that would result in shared benefits or costs for other Federal agencies or State or local governments;
5. Provides for identifying, for a proposed investment, quantifiable measurements for determining the net benefits and risks of the investment; and

6. Provides the means for senior management personnel of the Department to obtain timely information regarding the progress of an investment in an information system, including a system of milestones for measuring progress, on an independently verifiable basis, in terms of cost, capability of the system to meet specified requirements, timeliness and quality.

Institutionalizes performance-based and results-based management for information technology in coordination with the Chief Financial Officer (CFO) of the Department of Defense, the OSD Principal Staff Assistants, and the DoD Components and in accordance with Section 5123 of the ITMRA:

1. Establishes goals far improving the efficiency and effectiveness of DoD operations and, as appropriate, the delivery of services to the public through the effective use of information technology; and
2. Prescribes performance measurements for information technology used by or to be acquired for the Department that measure how well the information technology supports programs of the Department;

IAW Section 5126 of the ITMRA, prepares policies and procedures, in consultation with the CFO, to ensure that accounting, financial, and asset management systems and other information systems of DoD are designed, developed, and maintained to provide financial or program performance data for financial statements of the Department of Defense

Prepares guidance for budget formulation and congressional justification for information technology programs

Develops a departmental strategic plan that addresses the management and use of IT capabilities and prepares overall direction and guidance for managing DoD's information resources

Participates in CIO-led reviews of the information activities of the Department.

Oversees contracts that provide for multi-agency acquisitions of information technology in accordance with Section 5124 of the ITMRA and guidance issued by the Director of the Office of Management and Budget.

Provides oversight on Department-wide IT programs and activities to include:

- Information Work-force Training
- EC/EDI
- Directory Services
- Certificate Authorities
- Spectrum Policy and Oversight
- Encryption Policy

Director of Performance Assessments

In support of the CIO, DoD:

Assesses the results of performance-based and results-based management for information technology in coordination with the Chief Financial Officer, DoD, the OSD Principal Staff Assistants, the DoD Components and in accordance with Section 5123 of the ITMRA.

Where comparable processes and organizations in the public or private sectors exist, quantitatively benchmarks DoD process performance against such processes in terms of cost, speed, productivity, and quality of outputs and outcomes;

Prepares an annual report, to be included in the DoD budget submission to Congress, on the progress in achieving the goals;

Reviews and compiles information technology budget justification material, including the IT-43 Exhibit

IAW Section 5127 of the ITMRA, identifies any major information technology acquisition program, or any phase or increment of such a program, that has significantly deviated from the cost, performance, or schedule goals established for the program in the strategic information resources management plan required under Section 3506(b)(2) of Title 44, United States Code (Paperwork Reduction Act of 1995).

Monitors the performance of IT programs of the Department of Defense, evaluate the performance of those programs on the basis of applicable performance measurements, and recommends to the CIO when to advise the Secretary of Defense on whether to continue, modify, or terminate a program or project in accordance with Section 5125(c) (2) of the ITMRA.

Assesses, in consultation with the CFO, whether financial and related performance data are provided on a reliable, consistent, and timely basis to DoD financial management systems; and ensures that financial statements support:

Assessments and revisions of mission-related processes and administrative processes of the Department of Defense; and

Performance measurement of the performance in the case of investments made by the Department of Defense in information systems.

Coordinates with the offices, boards and Integrated Product Teams in OUSD(A&T) and the committees of the Defense Acquisition Board on the oversight and review of major automated information system acquisitions.

Serves as the Executive Secretary of CIO-led reviews of the information activities of the Department.

Prepares the agenda and other meeting materials and provide administrative support as needed.

Maintains records of CIO review decisions and assigned actions

Year 2000 Oversight

In support of the CIO, DoD:

Provides oversight and visibility into the Department's Year 2000 activities

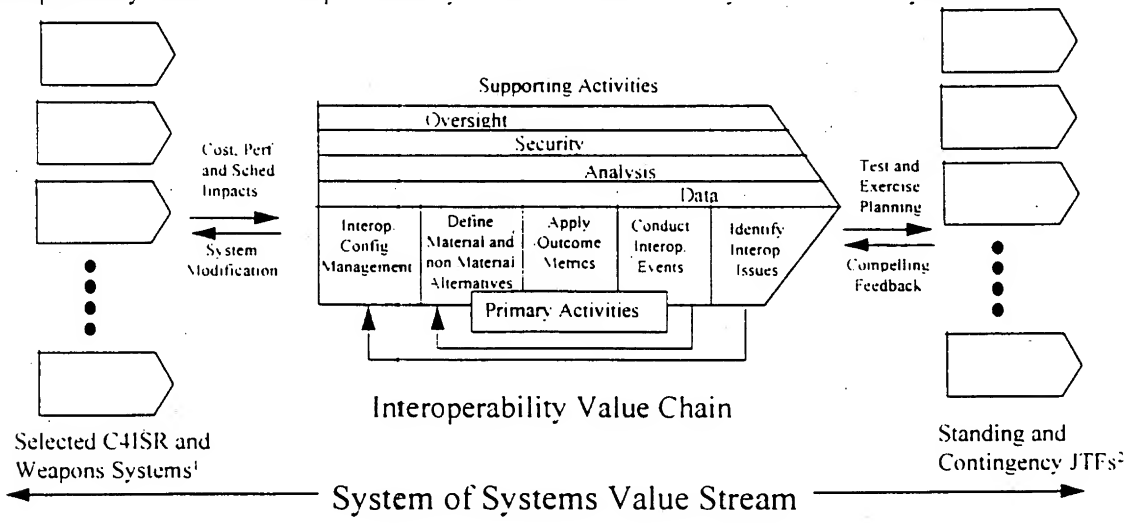
- Assessment
- Triage
- Conversions Strategies
- Remediation
- Tools
- Testing
- Resources

Provides oversight of and visibility into Contingency Planning for Functional Continuity

The following Interoperability White paper, prepared by CISA, is an excellent starting point for conducting systems-of-systems analysis. Although the paper highlights C4ISR systems, this process can be used to examine interoperability and data interfaces for information technology department-wide.

An Outcome Based Interoperability Improvement Process for the DoD

While there have been tangible gains achieved in the technical interoperability of C4ISR and associated weapons systems, these gains have been insufficient to satisfy the chronic shortfalls identified by combat and combat support personnel. The reasons for continued difficulties in achieving interoperability are complex and often obscured by organizational prerogatives and trans-organizational issues. These difficulties may have more to do with lack of a focused, realistic and comprehensive process for addressing interoperability within the DoD than any other single factor. The employment of outcome based metrics in conjunction with a more realistic economics benefit approach could provide a renewed focus and needed realism. The explicit coupling of requirements, systems acquisition and organizational training processes with interoperability determinations could ensure that interoperability issues were comprehensively addressed over the life cycles of critical systems.



Notes: 1. Systems selected based on CINC Operational Architectures

2. JTFs selected by JCS process

Figure 1. Outcome Based Interoperability Process

An outcome based interoperability process, such as depicted by figure one, works to focus the efforts of the DoD, not simply on the preparatory activities (e.g., specification preparation, RFP compliance), but more importantly on the tangible outcomes that would be expected based on the follow through of extant acquisition policies and operational tactics, techniques and procedures (TTP). Figure one describes an "interoperability value chain" which represents those primary activities that, in the context of interoperability, bear value in the outcome sense along with the necessary supporting activities which provide internal and external "horizontal" credibility to the value bearing activities. Horizontal supporting activities are essential to ensure that the interoperability value chain remains relevant in the larger DoD system of systems value stream.

Externally, this approach must be coupled to the acquisition process to ensure that those interoperability issues which have material solutions are coordinated within the acquisition community, the DoD Joint T&E process can be effectively leveraged and that Program Mangers are held accountable for those material solutions which gain the approval of the DoD Chief Information Officer (CIO), who would serve as the process owner. This approach

must also be coupled to Joint operations and training processes to ensure that exercises can be effectively leveraged and that non material solutions relating to doctrine and TTP are implemented. The role of the US Atlantic Command as the Joint Force Integrator is of special note in this regard -- especially given its recent acquisition of the Joint Battle Center.

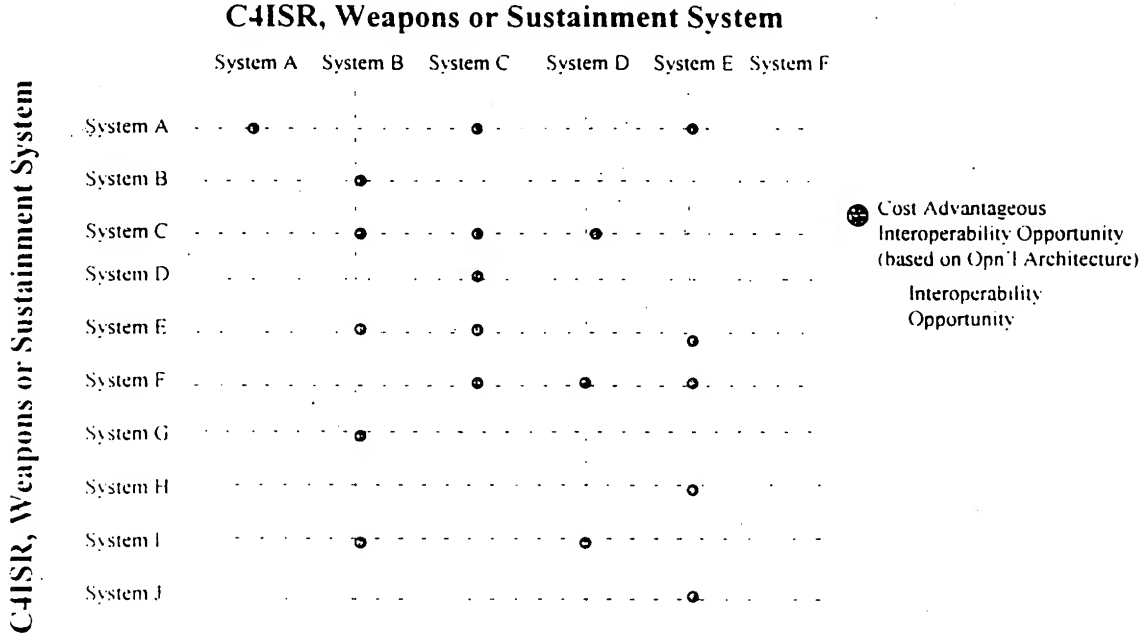


Figure 2. Interoperability Matrix Approach

It is impractical to expect universal interoperability -- especially given the constrained funding available for modernization and the length of time typically involved in fielding capabilities broadly across the force structure. Thus an "economic test" is necessary to allow the Department to allocate its resources on material and non material solutions to the highest value interoperability issues. As schematically depicted in figure two, there is are explicit benefits and costs associated with achieving interoperability among a set (i.e., two or more) systems within the larger system of systems. Sorting through the benefits and costs based on recognized warfighting needs and including Joint Vision 2010 will yield the necessary prioritization of the Departments interoperability efforts.

Of special importance to the utility of this process is the availability of outcome based metrics which can provide the evidentiary basis for demonstrating progress and illuminating residual interoperability or related issues. The development of these metrics (and their logical tie to the ITMRA and the GPRA) is a non trivial undertaking of the considerable importance. The role of metrics in this regard is to support the development of frequent and compelling feedback of a quality sufficient to be used to direct C4ISR and Weapons System Program Managers. Useful metrics should track to the accepted body of Joint tasks and TTP. The overall cost to the system of systems of tracking to these metrics during joint and service test and exercise events must be closely monitored to ensure the process does not become cost prohibitive in its own right. Some initial investment may be required as most test and exercise events are currently conducted with a fully stabilized C4ISR capability which is generally not stressed as a matter of exercise design and execution. Given the in excess of $45 Billion/year expended on C4ISR development, acquisition and operations and the clear trend to network centric warfare, a modest level of initial investment to revitalize what today is a process of marginal value is warranted.

Developing an outcome based approach to managing interoperability within the DoD comes as close as possible to "bottom line" management. It recognizes the equities of Program Managers while taking an effective step in achieving the required interoperability in the context of the Department's core function -- Joint Warfighting.